# Active Spread-Spectrum Steganalysis for Hidden Data Extraction

Ming Li
Dept. of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
mingli@buffalo.edu

Michel Kulhandjian
Dept. of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
mkk6@buffalo.edu

Dimitris A. Pados*
Dept. of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
pados@buffalo.edu

Stella N. Batalama
Dept. of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
batalama@buffalo.edu

Michael J. Medley
Air Force Research Laboratory/RITF
525 Brooks Rd
Rome, NY 13441
michael.medley@rl.af.mil

## ABSTRACT

This paper considers the problem of blind active spread-spectrum (SS) steganalysis defined as the extraction of hidden data with no prior information. We first develop a multi-signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown messages hidden in image hosts via multi-signature direct-sequence spread-spectrum embedding. Neither the original host nor the embedding signatures are assumed available. Then, cross-correlation enhanced M-IGLS (CC-M-IGLS), a procedure described herein in detail that is based on statistical analysis of repeated independent M-IGSL processing of the host, is seen to offer most effective hidden message recovery. In fact, experimental studies show that the proposed CC-M-IGLS active SS steganalysis algorithm can achieve probability of error close to what may be attained with known embedding signatures and host autocorrelation matrix.

## Categories and Subject Descriptors

D.2.11 [**Software Engineering**]: Software Architectures—*Information hiding*

## General Terms

Security, Algorithms, Theory

## Keywords

Blind detection, covert communications, data hiding, spread-spectrum embedding, steganalysis, steganography, watermarking

*Corresponding author.


*MMSEC 2011,* September 29–30, 2011, Buffalo, New York, USA.


## 1. INTRODUCTION

Steganography, which literally means "covered writing" in Greek, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio [1]-[3]. The basic purpose of steganography is to establish covert communication between trusting parties. While other data hiding applications (such as watermarking [4]-[6]) have their own individual requirements, the broad common objective of most steganographic applications is a satisfactory trade-off between hidden data resistance to noise/disturbance (robustness), information delivery rate (payload), and low host distortion for concealment purposes.

Steganalysis, which is the countermeasure technology to steganography, aims to discover the presence and/or extract the content of the secret data. Accordingly, steganalysis can be classified into two categories [7], *passive* and *active*. The primary task of passive steganalysis is to decide the presence or absence of hidden messages in given media objects. In contrast, active steganalysis refers to the effort of extracting the actual hidden data[1]. While passive steganalysis is being intensively investigated in the past few years [9]-[17], active steganalysis is a relatively new branch of research. To our best knowledge, there seems to have been little attempt in developing active steganalysis methods that can blindly extract the secret data.

In this work, we focus our attention on active spread-spectrum (SS) steganalysis. In particular, we aim to recover blindly secret data hidden in image hosts via (multi-signature) direct-sequence SS embedding [18]-[25]. Neither the original host nor the embedding signatures (spreading sequences) are known (fully blind SS steganalysis). In blind active SS steganalysis the unknown host acts as a source of interference/disturbance to the data to be extracted and, in a way, the problem parallels blind signal separation (BSS) applications as they arise

[1]In another interpretation of active steganalysis, the steganalyst manipulates the embedded data, such as introducing noise, in hopes of destroying the secret message (if any) [8].

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **SEP 2011** | | **00-00-2011 to 00-00-2011** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Active Spread-Spectrum Steganalysis For Hidden Data Extraction** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **State University of New York,Dept. of Electrical Engineering,Buffalo,NY,14260** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**To be presented at the 13th ACM Workshop on Multimedia and Security, Sep 29-30, 2011, Buffalo, NY, Government or Federal Purpose Rights License.**

14. ABSTRACT
**This paper considers the problem of blind active spreadspectrum (SS) steganalysis defined as the extraction of hidden data with no prior information. We first develop a multisignature iterative generalized least-squares (M-IGLS) core procedure to seek unknown messages hidden in image hosts via multi-signature direct-sequence spread-spectrum embedding. Neither the original host nor the embedding signatures are assumed available. Then, cross-correlation enhanced MIGLS (CC-M-IGLS), a procedure described herein in detail that is based on statistical analysis of repeated independent M-IGSL processing of the host, is seen to offer most effective hidden message recovery. In fact, experimental studies show that the proposed CC-M-IGLS active SS steganalysis algorithm can achieve probability of error close to what may be attained with known embedding signatures and host autocorrelation matrix.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **10** | |

in the fields of array processing, biomedical signal processing, and code-division multiple-access (CDMA) communication systems. Under the assumption that the embedded secret messages are independent identically distributed (i.i.d.) random sequences and independent to the cover host, independent component analysis (ICA) -one particular family of BSS methods- may be utilized to approach the hidden data extraction problem [7],[26]. However, ICA-based BBS algorithms degrade rapidly in the presence of correlated signal interference as is the case in SS image embedding. In [27], Gkizeli *et al.* developed an iterative generalized least squares (IGLS) procedure to blindly recover unknown messages hidden in image hosts via SS embedding. The algorithm has low complexity and remarkably good recovery performance. However, the scheme is designed solely for *single-signature* SS embedding where messages are hidden with one signature only. Realistically, a steganographer would favor *multi-signature* SS embedding to increase security and payload rate. The work in [27] is not generalizable to the *multi-signature* case.

In this paper, we develop a new *multi-signature* iterative generalized least squares (M-IGLS) SS steganalysis algorithm for hidden data extraction. For improved recovery performance, in particular for small hidden messages that pose the greatest challenge, we propose an algorithmic upgrade referred to as cross-correlation enhanced M-IGLS (CC-M-IGLS). CC-M-IGLS relies on statistical analysis of independent M-IGLS executions on the host and experimental studies indicate that can achieve hidden data recovery with probability of error close to what may be attained with known embedding signatures and known original host autocorrelation matrix.

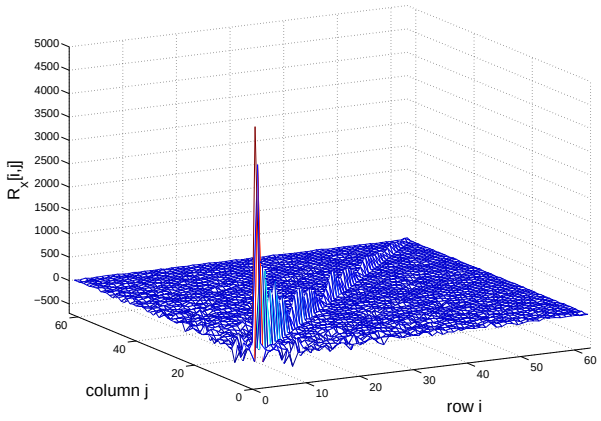
The rest of the paper is organized as follows. In Section 2 we present the signal model for the multi-signature SS embedding procedure and formulate the problem of active SS steganalysis. After developing the hidden data extraction algorithms in Section 3, experimental studies are presented in Section 4. Finally, some concluding remarks are drawn in Section 5.

The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real numbers; $()^T$ is the transpose operator; $\mathbf{I}_L$ is the $L \times L$ identity matrix; $\text{sgn}\{\cdot\}$ denotes zero-threshold quantization and $\mathbb{E}\{\cdot\}$ represents statistical expectation. Finally, $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$ are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

## 2. MULTI-SIGNATURE SS EMBEDDING AND STEGANALYSIS PROBLEM FORMULATION

Consider a host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\mathbf{H}$ is partitioned into $M$ local non-overlapping blocks of size $\frac{N_1 N_2}{M}$. Each block, $\mathbf{H}_1, \mathbf{H}_2, ...., \mathbf{H}_M$, is to carry $K$ hidden information bits coming -potentially- from $K$ distinct messages. Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform, a wavelet transform, etc.). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_m) \in \mathbb{R}^{\frac{N_1 N_2}{M}}, m = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_m)$ we choose a fixed subset of $L \leq \frac{N_1 N_2}{M}$ coefficients (bins) to form the final host vectors $\mathbf{x}(m) \in \mathbb{R}^L$, $m = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

(a)




(b)

**Figure 1: (a) Baboon image example $\mathbf{H} \in \{0, 1, ..., 255\}^{256 \times 256}$. (b) Host data autocorrelation matrix ($8 \times 8$ DCT, 63-bin host).**

The autocorrelation matrix of the host data $\mathbf{x}$ is an important statistical quantity for our developments and is defined as $\mathbf{R}_\mathbf{x} \triangleq \mathbb{E}\{\mathbf{x}\mathbf{x}^T\} = \frac{1}{M}\sum_{m=1}^{M} \mathbf{x}(m)\mathbf{x}(m)^T$. It is easy to verify that in general $\mathbf{R}_\mathbf{x} \neq \alpha \mathbf{I}_L, \alpha > 0$; that is, $\mathbf{R}_\mathbf{x}$ is *not* constant-value diagonal or "white" in field language. For example, $8 \times 8$ DCT with 63-bin host data formation (excluding only the dc coefficient) for the $256 \times 256$ gray-scale Baboon image in Fig. $1(a)$ gives the host autocorrelation matrix $\mathbf{R}_\mathbf{x}$ in Fig. $1(b)$.

### 2.1 Multi-signature SS Embedding

The $K$ distinct message bit sequences $\{b_k(m)\}_{m=1}^M$, $k = 1, 2, \ldots, K$, $b_k(m) \in \{\pm 1\}$, are hidden in the transform-domain host vectors $\{\mathbf{x}(m)\}_{m=1}^M$ via additive SS embedding by means of $K$ spreading sequences (signatures) $\mathbf{s}_k \in$

$\mathbb{R}^L, \|\mathbf{s}_k\| = 1,\ k = 1, 2, \ldots, K,$

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m),\ m = 1, 2, \ldots, M, \quad (1)$$

with corresponding amplitudes $A_k > 0,\ k = 1, \ldots, K$; for the sake of generality, $\mathbf{n}(m) \sim \mathcal{N}(\mathbf{0}, \sigma_n^2 \mathbf{I}_L)$ represents potential external white Gaussian noise[2] with variance $\sigma_n^2$. It is assumed that $b_k(m)$ behave as equi-probable binary random variables that are independent in time, $m = 1, ..., M$, and across messages, $k = 1, ..., K$. The contribution of each individual embedded message bit $b_k$ to the composite signal is $A_k b_k \mathbf{s}_k$ and the mean-squared distortion to the original host data $\mathbf{x}$ due to the embedded $k$ message alone is

$$\mathcal{D}_k = \mathbb{E}\{\|A_k \mathbf{s}_k b_k\|^2\} = A_k^2,\ \ k = 1, 2, ..., K. \quad (2)$$

Under statistical independence of messages, the mean-squared distortion of the original image due to the total, multi-message, insertion is $\mathcal{D} = \sum_{k=1}^{K} A_k^2$.

The intended recipient of the $k$th message can perform hidden bit detection by looking at the sign of the output of the minimum-mean-square-error (MMSE) filter $\mathbf{w}_{MMSE,k}$:

$$\hat{b}_k(m) = \mathrm{sgn}\{\mathbf{w}_{MMSE,k}^T \mathbf{y}(m)\} = \mathrm{sgn}\{\mathbf{s}_k^T \mathbf{R}_{\mathrm{y}}^{-1} \mathbf{y}(m)\} \quad (3)$$

where $\mathbf{R}_{\mathrm{y}}$ is the autocorrelation matrix of the stego vectors $\{\mathbf{y}(m)\}_{m=1}^{M}$

$$\mathbf{R}_{\mathrm{y}} \triangleq \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{R}_{\mathrm{x}} + \sum_{k=1}^{K} A_k^2 \mathbf{s}_k \mathbf{s}_k^T + \sigma_n^2 \mathbf{I}_L. \quad (4)$$

The autocorrelation matrix $\mathbf{R}_{\mathrm{y}}$ can be estimated by sample averaging over the finite set of $M$ stego data, $\widehat{\mathbf{R}}_{\mathrm{y}} = \frac{1}{M}\sum_{m=1}^{M} \mathbf{y}(m)\mathbf{y}(m)^T$. Using $\widehat{\mathbf{R}}_{\mathrm{y}}$ in (3), we obtain what is known as the sample-matrix-inversion MMSE (SMI-MMSE) detector implementation [28].

## 2.2 Formulation of Active Steganalysis Problem

We assume that the active extraction steganalyst has the ability to obtain transform domain stego data in the form of $\mathbf{y}(m)$ in (1) after performing appropriate image partition, transform, and coefficient selection[3] on the image classified as stego by passive steganalysis. We denote the combined "disturbance" to the hidden data (host plus noise) by $\mathbf{z}(m) \triangleq \mathbf{x}(m) + \mathbf{n}(m)$. Then, SS embedding by (1) can be rewritten as

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{z}(m),\ m = 1, \ldots, M, \quad (5)$$

where $\mathbf{z}(m)$ is modeled as a sequence of zero-mean (without loss of generality) vectors with autocovariance matrix $\mathbf{R}_{\mathrm{z}} = \mathbb{E}\{\mathbf{z}\mathbf{z}^T\} = \mathbf{R}_{\mathrm{x}} + \sigma_n^2 \mathbf{I}$. Let $\mathbf{v}_k \triangleq A_k \mathbf{s}_k \in \mathbb{R}^L$, $k = 1, \ldots, K$, be amplitude-including embedding signatures. Then, we can further rewrite SS embedding as

$$\begin{aligned} \mathbf{y}(m) &= \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{z}(m) & (6)\\ &= \mathbf{V}\mathbf{b}(m) + \mathbf{z}(m),\ m = 1, \ldots, M, & (7) \end{aligned}$$

where $\mathbf{V} \triangleq [\mathbf{v}_1, \ldots, \mathbf{v}_K] \in \mathbb{R}^{L \times K}$ is the amplitude-including signature matrix and $\mathbf{b}(m) \in \{\pm 1\}^{K \times 1}$ is the vector of bits embedded in the $m$th host block. For notational simplicity, we can write the whole stego image data as one matrix

$$\mathbf{Y} = \mathbf{V}\mathbf{B} + \mathbf{Z} \quad (8)$$

where $\mathbf{Y} \triangleq [\mathbf{y}(1)\mathbf{y}(2)...\mathbf{y}(M)] \in \mathbb{R}^{L \times M}$, $\mathbf{B} \triangleq [\mathbf{b}(1)\mathbf{b}(2)...\mathbf{b}(M)] \in \{\pm 1\}^{K \times M}$, and $\mathbf{Z} \triangleq [\mathbf{z}(1)\ \mathbf{z}(2)\ ...\ \mathbf{z}(M)] \in \mathbb{R}^{L \times M}$.

Our objective is to blindly extract the unknown hidden data $\mathbf{B}$ from the stego data $\mathbf{Y}$ without prior knowledge of the embedding signatures $\mathbf{s}_k$, and amplitudes $A_k$, $k = 1, \ldots, K$, in $\mathbf{V} = [A_1\mathbf{s}_1, \ldots, A_k\mathbf{s}_k]$ or the host itself $\mathbf{x}(1), \ldots, \mathbf{x}(M)$ in $\mathbf{Z} = [\mathbf{x}(1) + \mathbf{n}(1), \ldots, \mathbf{x}(M) + \mathbf{n}(M)]$.

# 3. ACTIVE STEGANALYSIS FOR HIDDEN DATA EXTRACTION

If $\mathbf{Z}$ were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of $\mathbf{V}$ and detector of $\mathbf{B}$ would be

$$\widehat{\mathbf{V}}, \widehat{\mathbf{B}} = \arg \min_{\substack{\mathbf{B} \in \{\pm 1\}^{(K \times M)}, \\ \mathbf{V} \in \mathbb{R}^{L \times K}}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2 \quad (9)$$

where multiplication by $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$ can be interpreted as prewhitening of the compound observation data. If Gaussianity of $\mathbf{Z}$ is not to be invoked, then (9) is simply referred to as the joint generalized least-squares (GLS) solution[4] of $\mathbf{V}$ and $\mathbf{B}$.

## 3.1 Multi-signature Iterative Generalized Least-Squares Procedure

The global GLS-optimal message matrix $\widehat{\mathbf{B}}$ in (9) can be computed independently of $\widehat{\mathbf{V}}$ by exhaustive search over all possible choices under the criterion function $\|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2$,

$$\widehat{\mathbf{B}} = \arg \min_{\mathbf{B} \in \{\pm 1\}^{K \times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2 \quad (10)$$

where $\mathbf{P}_{\perp\mathbf{B}} \triangleq \mathbf{I} - \mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B}$. Exhaustive search has, of course, complexity exponential in $KM$ (total size of hidden messages in bits). We consider this cost unacceptable and attempt to reach a quality approximation of the solution of (10) (or (9), to that respect) by alternating generalized least-squares estimates of $\mathbf{V}$ and $\mathbf{B}$, iteratively, as described below.

Pretend $\mathbf{B}$ is known; the generalized least-squares estimate

[2]Additive white Gaussian noise is frequently viewed as a suitable model for quantization errors, channel transmission disturbances, and/or image processing attacks.

[3]Host image partition may be estimated by examining the difference between neighboring pixels [14]. For each investigated transform, all coefficients (except the dc value) may be considered.

[4]Generalized-least squares solutions are weighted least-squares (WLS) solutions with optimal weighting matrices, here $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$, that yield the lowest variance of the estimation error [31],[34].

of $\mathbf{V}$ is

$$\begin{aligned}\widehat{\mathbf{V}}_{\rm GLS} &= \arg\min_{\mathbf{V}\in\mathbb{R}^{L\times K}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &= \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \end{aligned} \quad (11)$$

Pretend, in turn, that $\mathbf{V}$ is known; then, the least-squares estimate of $\mathbf{B}$ *over the real field* is

$$\begin{aligned}\widehat{\mathbf{B}}_{\rm GLS}^{\rm real} &= \arg\min_{\mathbf{B}\in\mathbb{R}^{K\times M}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &= (\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{Y}. \end{aligned} \quad (12)$$

Observing that

$$(\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm z}^{-1} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}, \quad (13)$$

we rewrite

$$\widehat{\mathbf{B}}_{\rm GLS}^{\rm real} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y} \quad (14)$$

and suggest the approximate binary message solution

$$\begin{aligned}\widehat{\mathbf{B}}_{\rm GLS}^{\rm binary} &= \arg\min_{\mathbf{B}\in\{\pm1\}^{K\times M}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &\simeq {\rm sgn}\{(\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y}\}. \end{aligned} \quad (15)$$

The proofs of (11), (12), and (13) are provided in the appendix.

The *multi-signature iterative generalized least-squares* (M-IGLS) procedure suggested by the two equations (11) and (15) is now straightforward. Initialize $\widehat{\mathbf{B}}$ arbitrarily and alternate iteratively between (11) and (15) to obtain at each step conditionally generalized least squares estimates of one matrix parameter given the other. Stop when convergence is observed. Notice that (15) requires knowledge of the autocorrelation matrix of the stego data $\mathbf{R}_{\rm y}$ which can be estimated by sample averaging over the received data observations, $\widehat{\mathbf{R}}_{\rm y} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{y}(m)\mathbf{y}(m)^T$. The M-IGLS SS steganalysis algorithm is summarized in Table 1. Superscripts denote iteration index. For the sake of mathematical accuracy, we emphasize that there is always a sign/phase ambiguity present when one considers joint data extraction and signature identification. The sign ambiguity problem can be overcome with a few known or guessed data symbols for sign correction.

## 3.2 Cross-Correlation Enhanced M-IGLS

We understand that, with arbitrary initialization, convergence of the M-IGLS procedure described in Table 1 to the optimal GLS solution of (9) is not guaranteed in general. Extensive experimentation with the algorithm in Table 1 indicates that, for sufficiently long messages hidden by each signature ($M$ = 4Kbits or more, for example), satisfactory quality message decisions $\widehat{\mathbf{B}}$ can be obtained. However, when the message size is small, M-IGLS may very well converge/return wrong solutions. The quality (generalized-least-squares fit) of the end convergence point depends heavily on the initialization point and arbitrary initialization - which at first sight is unavoidable for blind steganalysis- offers little assurance that the iterative scheme will lead us to appropriate, "reliable" (close to minimal generalized least-squares fit) solutions. Re-initialization and re-execution of the M-IGLS procedure is always possible but the challenge

**Table 1: Iterative generalized least-squares SS steganalysis**

1) $d := 0$; initialize $\widehat{\mathbf{B}}^{(0)} \in \{\pm1\}^{K\times M}$ arbitrarily.
2) $d := d+1$;
$\widehat{\mathbf{V}}^{(d)} := \mathbf{Y}(\widehat{\mathbf{B}}^{(d-1)})^T\left[(\widehat{\mathbf{B}}^{(d-1)})(\widehat{\mathbf{B}}^{(d-1)})^T\right]^{-1}$;
$\widehat{\mathbf{B}}^{(d)} := {\rm sign}\left\{\left((\widehat{\mathbf{V}}^{(d)})^T\widehat{\mathbf{R}}_{\rm y}^{-1}(\widehat{\mathbf{V}}^{(d)})\right)^{-1}(\widehat{\mathbf{V}}^{(d)})^T\widehat{\mathbf{R}}_{\rm y}^{-1}\mathbf{Y}\right\}$.
3) Repeat Step 2 until $\widehat{\mathbf{B}}^{(d)} = \widehat{\mathbf{B}}^{(d-1)}$.

is how to assess whether solutions returned by the M-IGLS procedure are reliable or not without any side information. The rest of this section is devoted to addressing this challenge.

Since $\widehat{\mathbf{B}}$ and $\widehat{\mathbf{V}}$ are jointly detected and estimated, correspondingly, if one is not reliable neither is the other in general. We first examine the reliability of the bit matrix decision $\widehat{\mathbf{B}} = [\widehat{\mathbf{b}}_1,\ldots,\widehat{\mathbf{b}}_K]^T$ returned by the M-IGLS procedure of Table 1. The sample cross-correlation between any two bit streams is

$$\eta_{i,j} \triangleq \widehat{\mathbf{b}}_i^T\widehat{\mathbf{b}}_j/M,\ i\neq j,\ i,j=1,\ldots,K. \quad (16)$$

Formally, the true information bits are independent within user streams and across users. If $\eta_{i,j}$ were to be viewed as approximately normally distributed with zero mean and variance $\frac{1}{M}$, then the probability of $|\eta_{i,j}|$, $i\neq j$, being larger than, say, the threshold value $\frac{3}{\sqrt{M}}$ is very low at about 0.3% (we can calculate $\Pr(|\eta_{i,j}| > \frac{3}{\sqrt{M}}) \approx 0.003$). Motivated by this calculation, we introduce below Criterion 1 that classifies convergence points of the M-IGLS procedure in Table 1 as "compliant" or not based on the sample statistics of the returned data matrix $\widehat{\mathbf{B}}$.

*Criterion 1:* If $|\eta_{i,j}| \leq \frac{3}{\sqrt{M}}$ for all $i\neq j\in\{1,2,\ldots,K\}$, then $(\widehat{\mathbf{B}},\widehat{\mathbf{V}})$ returned by the M-IGLS procedure in Table 1 are classified as "*Criterion-1-compliant.*" ■

Criterion 1 provides the means for coarse identification of unreliable solutions. An unreliable convergence point would then trigger re-initialization and re-execution of the M-IGLS procedure in Table 1 until a Criterion-1-compliant point is obtained. To enhance the end accuracy of blind hidden data extraction, we propose one additional criterion based on the returned estimated signature matrix $\widehat{\mathbf{V}}$. We will motivate our proposal by examining experimentally the normalized cross-correlation between the estimated signatures $\widehat{\mathbf{v}}_k$ returned by the Criterion-1-equipped M-IGLS procedure and the true signatures $\mathbf{v}_k$, $k=1,\ldots,K$. We consider as a host example the gray scale $256\times256$ "Baboon" image of Fig. 1(a) and perform $8\times8$ block DCT embedding by (1) over all bins except the dc coefficient with $K=4$ distinct arbitrary signatures $\mathbf{s}_k\in\mathbb{R}^{63}$ and per-message distortion $\mathcal{D}_k$ = 31.5dB, $k=1,\ldots,4$. For the sake of generality, we also incorporate white Gaussian noise of variance $\sigma_n^2$ = 3dB. We run the Criterion-1-equipped M-IGLS procedure 400 times. The histogram of the normalized cross-correlation values $\theta_k \triangleq \frac{\widehat{\mathbf{v}}_k^T\mathbf{v}_k}{\|\widehat{\mathbf{v}}_k\|\|\mathbf{v}_k\|}$ of the four hundred returned solutions for message $k=1$ in Fig. 2 (representative of all other messages) reveals that Criterion 1 is not by itself sufficient to

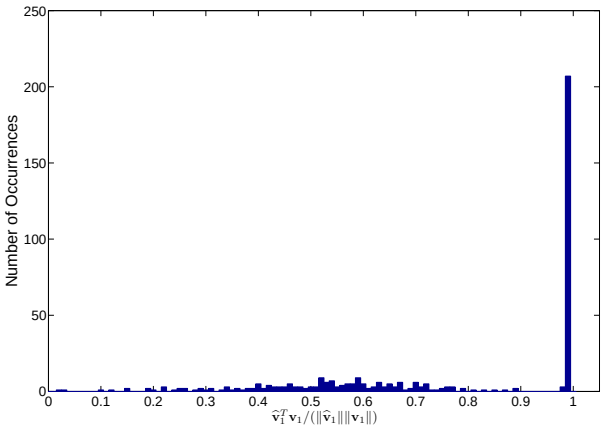



**Figure 2: Histogram of normalized cross-correlation between $\widehat{\mathbf{v}}_1$ and $\mathbf{v}_1$ ($256 \times 256$ Baboon image, $8 \times 8$ DCT, $L = 63$, $K = 4$, $\mathcal{D}_k = 31.5$dB, $k = 1, \ldots, 4$, $\sigma_n^2 =$ 3dB; $\widehat{\mathbf{v}}_1$ returned by Table 1 M-IGLS steganalysis procedure).**

eliminate erroneous solutions. Yet, there exists a tight cluster/region formed by 210 or so of the Criterion-1-equipped M-IGLS convergence points around the true embedding signature.

The basic idea now behind our second and final refinement of the M-IGLS blind hidden data extraction procedure is to identify and average these reliable clustered estimates. Of course, identification of the reliable estimates is not a trivial task due to our complete lack of knowledge of $\mathbf{v}_k$ (or $\mathbf{s}_k$), $k = 1, \ldots, K$. In this context, assume that we have $P$ estimates of $\mathbf{v}_k$ denoted by $\widehat{\mathbf{v}}_k^{(j)}$, $k = 1, \ldots, K$, $j = 1, \ldots, P$, obtained by $P$ runs of the Criterion-1-equipped M-IGLS procedure. From the example of Fig. 2, we understand that reliable estimates $\widehat{\mathbf{v}}_k^{(j)}$ of $\mathbf{v}_k$ have high normalized cross-correlation (close to 1) with each other, while they will have low normalized cross-correlation with other unreliable estimates of $\mathbf{v}_k$. In contrast, unreliable estimates will tend to have low normalized cross-correlation with each other. Therefore, the reliability of $\widehat{\mathbf{v}}_k^{(j)}$ may be quantified/assessed by examining the sum-cross-correlation with the other $\widehat{\mathbf{v}}_k^{(t)}$, $t \neq j \in \{1, \ldots, P\}$,

$$\rho_k^{(j)} \triangleq \sum_{t=1, t\neq j}^{P} \frac{|\widehat{\mathbf{v}}_k^{(j)H}\widehat{\mathbf{v}}_k^{(t)}|}{\|\widehat{\mathbf{v}}_k^{(j)}\|\|\widehat{\mathbf{v}}_k^{(t)}\|} \,. \tag{17}$$

A reasonable threshold value for binary reliability classification may be the average value

$$\overline{\rho}_k \triangleq \frac{1}{P}\sum_{j=1}^{P} \rho_k^{(j)}, \;\; k = 1, \ldots, K, \tag{18}$$

utilized in the proposed Criterion 2 below.

*Criterion 2:* Let $\widehat{\mathbf{v}}_k^{(j)}$ be the estimates of $\mathbf{v}_k$ returned by $P$ arbitrary initializations of the Criterion-1-equipped M-IGLS procedure of Table 1, $k = 1, \ldots, K$, $j = 1, \ldots, P$. If $\rho_k^{(j)} \geq \overline{\rho}_k$, then $\widehat{\mathbf{v}}_k^{(j)}$ is considered a *reliable* estimate of the $\mathbf{v}_k$; otherwise we declare it as *unreliable*. ■

**Table 2: Cross-correlation Enhanced M-IGLS**

**For** $j := 1$ to $P$
1) Execute M-IGLS of Table 1 with arbitrary initialization and obtain estimates $\widehat{\mathbf{v}}_k$, $k = 1, \ldots, K$.
2) **If** estimates are Criterion-1-compliant, $\widehat{\mathbf{v}}_k^{(j)} := \widehat{\mathbf{v}}_k$, $k = 1, \ldots, K$; **else** go to 1).

**End**

**For** $k := 1$ to $K$
3) Identify reliable estimates for $\mathbf{v}_k$ according to *Criterion 2*.
4) Calculate the average over all reliable estimates $\overline{\widehat{\mathbf{v}}}_k$ by (19).

**End**

5) Set $\overline{\widehat{\mathbf{V}}} \triangleq [\overline{\widehat{\mathbf{v}}}_1, \ldots, \overline{\widehat{\mathbf{v}}}_K]$.
6) Execute M-IGLS of Table 1 with initialization $\widehat{\mathbf{B}}^{(0)} = \text{sgn}\left\{\left(\overline{\widehat{\mathbf{V}}}^T\widehat{\mathbf{R}}_{\text{y}}^{-1}\overline{\widehat{\mathbf{V}}}\right)^{-1}\overline{\widehat{\mathbf{V}}}^T\widehat{\mathbf{R}}_{\text{y}}^{-1}\mathbf{Y}\right\}$.

Finally, we average our reliable (according to *Criterion 2*) estimates of the effective signatures $\mathbf{v}_k$ to produce one last high-quality initialization of the M-IGLS algorithm of Table 1. Let $\mathcal{S}_k$ denote the set of all reliable estimates of $\mathbf{v}_k$ according to *Criterion 2* and let $|\mathcal{S}_k|$ denote the cardinality of $\mathcal{S}_k$. Our averaged estimate of matrix $\mathbf{V}$ is now given by $\overline{\widehat{\mathbf{V}}}$ with

$$\overline{\widehat{\mathbf{V}}} \triangleq \left[\overline{\widehat{\mathbf{v}}}_1, \ldots, \overline{\widehat{\mathbf{v}}}_K\right] \;\; \text{where} \;\; \overline{\widehat{\mathbf{v}}}_k = \frac{1}{|\mathcal{S}_k|}\sum_{j\in\mathcal{S}_k}\widehat{\mathbf{v}}_k^{(j)} \;, \; k = 1 \ldots, K, \tag{19}$$

i.e. $\overline{\widehat{\mathbf{v}}}_k$ is the average over all reliable estimates of $\mathbf{v}_k$ according to *Criterion 2*. We execute M-IGLS in Table 1 a final time initialized at $\widehat{\mathbf{B}}^{(0)} = \text{sgn}\left\{\left(\overline{\widehat{\mathbf{V}}}^T\widehat{\mathbf{R}}_{\text{y}}^{-1}\overline{\widehat{\mathbf{V}}}\right)^{-1}\overline{\widehat{\mathbf{V}}}^T\widehat{\mathbf{R}}_{\text{y}}^{-1}\mathbf{Y}\right\}$. We call M-IGLS with both Criteria 1 and 2 incorporated, Cross-Correlation enhanced M-IGLS (CC-M-IGLS) and summarize the complete procedure in Table 2.

# 4. EXPERIMENTAL STUDIES

A technically firm and keen measure of quality of an active steganalysis solution is the difference in the bit-error-rate (BER) experienced by the intended recipient and the steganalyst. The intended recipient in our studies may be using any of the following three message recovery methods: (*i*) Standard signature matched-filtering (MF) with the known signatures $\mathbf{s}_k$, $k = 1, ..., K$, (*ii*) sample-matrix-inversion MMSE (SMI-MMSE) filtering with known signatures $\mathbf{s}_k$ and estimated host autocorrelation matrix $\widehat{\mathbf{R}}_{\text{y}}$ (see (3)); (*iii*) ideal MMSE filtering with known signatures $\mathbf{s}_k$ and known true host autocorrelation matrix $\mathbf{R}_{\text{x}}$ which serves as the ultimate performance bound reference for all methods. In terms of blind active steganalysis (neither $\mathbf{s}_k$ nor $\mathbf{R}_{\text{x}}$ known), we will examine (*iv*) the developed M-IGLS algorithm in Table 1 alone and (*v*) CC-M-IGLS of Table 2 with $P = 20$ Criterion-1 runs. Finally, the performance of two typical ICA-based blind signal separation (BSS) algorithms, (*vi*) FastICA [35], and (*vii*) JADE [36], will also be included in the studies for comparison purposes.

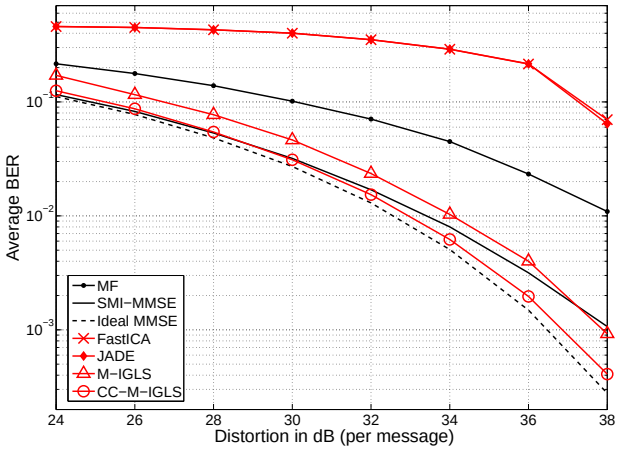



**Figure 3: Average BER versus per-message distortion ($512 \times 512$ Baboon, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB).**

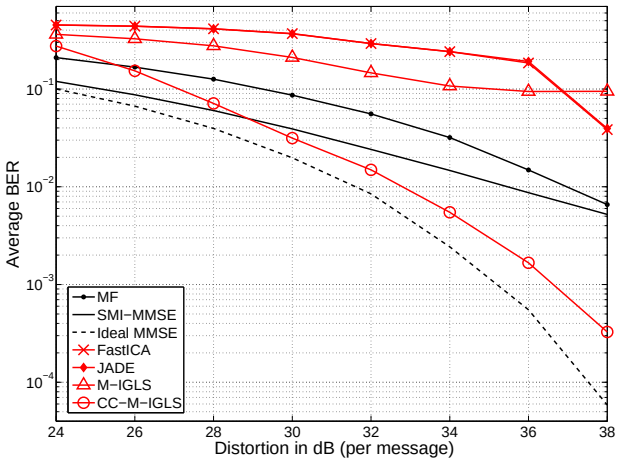



**Figure 4: Average BER versus per-message distortion ($256 \times 256$ Baboon, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB).**

We first consider as a host example the gray-scale $512 \times 512$ "Baboon" image. We perform $8 \times 8$ block DCT embedding by (1) over all bins except the dc coefficient with $K = 4$ distinct arbitrary signatures $\mathbf{s}_k \in \mathbb{R}^{63}$, $k = 1, \ldots, K$. The hidden message embedded by each signature is $\frac{512^2}{8^2} = 4,096$ bits long. The per-message mean square distortion due to each embedded message is set to be the same for all messages, i.e. $\mathcal{D}_k = A_k^2 = \frac{\mathcal{D}}{K}$, $k = 1, \ldots, 4$. For the sake of generality, we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$dB. Fig. 3 shows the average BER (over all $K = 4$ messages) of all methods $(i)$ through $(vii)$ listed above as a function of the host distortion per message. While the independent/principal-component methods (FastICA and JADE) are failing to carry out effective active SS image steganalysis, to our satisfaction CC-M-IGLS SS steganalysis is rather close in BER performance to the ideal MMSE detector bound where both the embedding signatures and the clean host autocorrelation matrix $\mathbf{R}_x$ are perfectly known. It could be argued that for this host and

**Figure 5: $512 \times 512$ gray-scale Boat image.**

rather large size of $M = 4,096$ bits per message, CC-M-IGLS offers a moderate gain only in comparison with M-IGLS of Table 1 by itself.

In Fig. 4, however, we repeat the exact same experimental study on the smaller $256 \times 256$ version of the Baboon image Fig. $1(a)$ with $K = 4$ hidden messages of length only $\frac{256^2}{8^2} = 1,024$ bits per message. CC-M-IGLS now provides dramatic performance improvement over M-IGLS which surely justifies the extra computational cost and extraction delay. At the same time, comparing with Fig. 3, the gap between CC-M-IGLS and ideal MMSE increases as the hidden message size (use of signature, individually) decreases.

For additional experimental validation, the studies of Fig. 3 and Fig. 4 are repeated on the familiar "Boat" image (shown in Fig. 5) in its $512 \times 512$ and $256 \times 256$ gray-scale versions (Fig. 6 and Fig. 7, correspondingly). Identical conclusions are drawn regarding the effectiveness of CC-M-IGLS blind active steganalysis.

Finally, to examine the behavior of CC-M-IGLS under increased-density small-message hiding, we consider the $256 \times 256$ gray-scale "F-16 Aircraft" image (shown in Fig. 8) with $K = 4$ or $K = 8$ hidden messages of length 1Kbit each. Recovery performance plots are given in Fig. 9 and Fig. 10, correspondingly. An encompassing conclusion over all executed experiments is that CC-M-IGLS remains a most effective technique to extract blindly hidden messages, while extraction becomes more challenging as the length of hidden messages (use of an embedding signature) decreases or the number of hidden messages (number of used signatures) increases.

## 5. CONCLUSIONS

In this paper we considered the problem of active blind spread-spectrum steganalysis and attempted to recover unknown messages hidden in image hosts via multi-signature spread-spectrum embedding. Neither the original host nor the embedding signatures are assumed available. We first

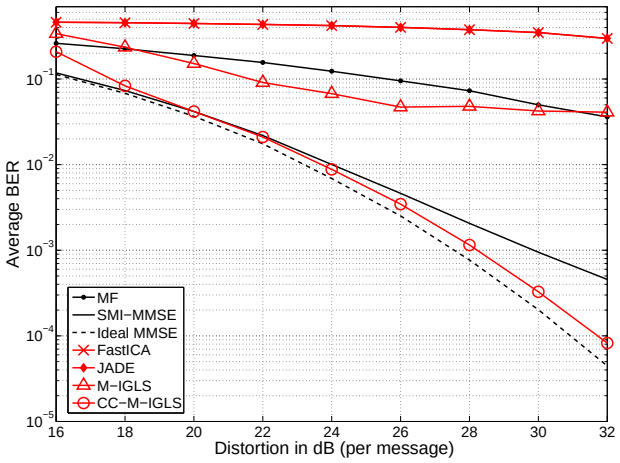



**Figure 6: Average BER versus per-message distortion ($512\times512$ Boat, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB).**

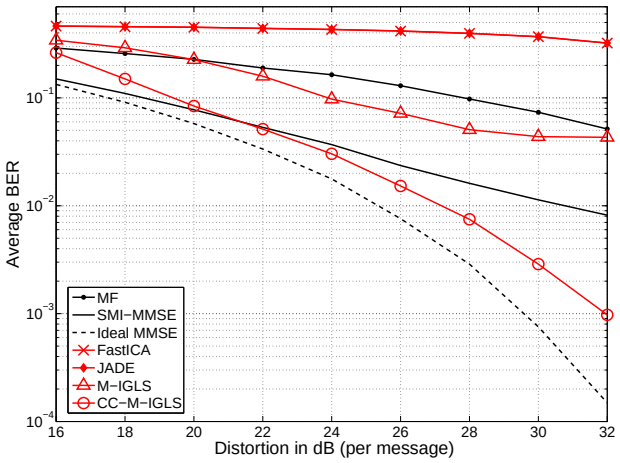



**Figure 7: Average BER versus per-message distortion ($256\times256$ Boat, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB).**

**Figure 8: $256 \times 256$ gray-scale Aircraft image.**

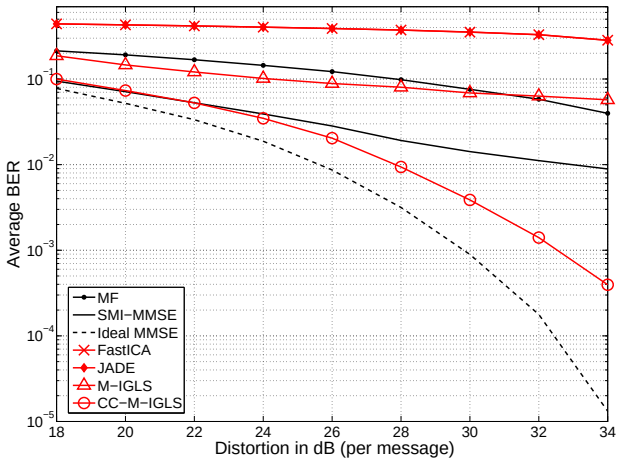



**Figure 9: Average BER versus per-message distortion ($256 \times 256$ Aircraft, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB).**

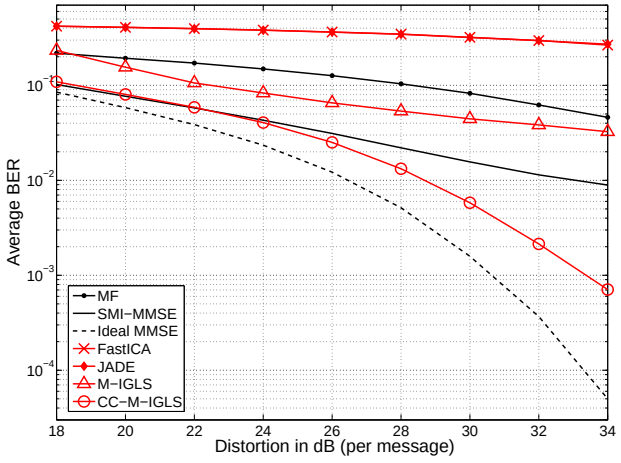



**Figure 10: Average BER versus per-message distortion ($256 \times 256$ Aircraft, $L = 63$, $K = 8$ messages of 1Kbit each, $\sigma_n^2 = 3$dB).**

developed a low complexity multi-signature iterative generalized least-squares (M-IGLS) core algorithm. Cross-correlation enhanced M-IGLS (CC-M-IGLS), a procedure based on statistical analysis of repeated independent M-IGLS processing of the host, offers most effective blind hidden message recovery. In fact, experimental studies showed that CC-M-IGLS can achieve probability of error rather close to what may be attained with known embedding signatures and known original host autocorrelation matrix and present ifself as an efficient countermeasure to conventional[5] SS steganography.

[5]In [26], Bas and Cayre present an interesting signature-based additive embedding approach different to (1) that is host-vector-by-host-vector dependent and would withstand IGLS-based active stegnalysis. The embedding is, however, very sensitive to noise that would lead to high recovery error rates by intended recipients and limit the applicability to general covert communication problems.

## 6. REFERENCES


[1] N. F. Johnson and S. Katzenbeisser. A survey of steganographic techniques. In S. Katzenbeisser and F. Petitcolas, editors, *Information Hiding*, pages 43-78. Norwood, MA: Artech House, 2000.

[2] S. Wang and H. Wang. Cyber warfare: Steganography vs. steganalysis. *Communications of the ACM*, 47(10):76-82, Oct. 2004.

[3] C. Cachin. An information-theoretic model for steganography. In *Proc. 2nd Intern. Workshop Information Hiding*, pages 306-318. Portland, OR, Apr. 1998.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[5] F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proc. IEEE*, 87(7):1079-1107, July 1999.

[6] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk. Watermarking digital image and video data: A state-of-the-art overview. *IEEE Signal Processing Magazine*, 17(5):20-46, Sept. 2000.

[7] R. Chandramouli. A mathematical framework for active steganalysis. *ACM Multimedia Systems Special Issue on Multimedia Watermarking*, 9(3):303-311, Sept. 2003,

[8] Y. Wang and P. Moulin. Perfectly secure steganography: Capacity, error exponents, and code constructions. *IEEE Trans. Inform. Theory*, 54(6):2706-2722, June 2008.

[9] S. Lyu, and H. Farid. Steganalysis using higher-order image statistics. *IEEE Trans. Inform. Forensics and Security*, 1(1):111-119, Mar. 2006.

[10] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. Steganalysis for Markov cover data with applications to images. *IEEE Trans. Inform. Forensics and Security*, 1(2):275-287, June 2006.

[11] İ. Avcıbaş, N. Memon, and B. Sankur. Steganalysis using image quality metrics. *IEEE Trans. Image Proc.*, 12(2):221-229, Feb. 2003.

[12] W. Lie and G. Lin. A feature-based classification technique for blind image steganalysis. *IEEE Trans. Multimedia*, 7(6):1007-1020, Dec. 2005.

[13] G. Gul and F. Kurugollu. SVD-based universal spatial domain image steganalysis. *IEEE Trans. Inform. Forensics and Security*, 5(2):349-353, June 2010.

[14] Y. Wang and P. Moulin. Steganalysis of block-DCT image steganography. In *Proc. IEEE Workshop on Statistical Signal Processing*, pages 339-342. Saint-Louis, MO, Sept. 2003.

[15] Y. Wang and P. Moulin. Optimized feature extraction for learning-based image steganalysis. *IEEE Trans. Inform. Forensics and Security*, 2(1):31-45, Mar. 2007.

[16] B. Li, J. Huang, and Y. Q. Shi. Steganalysis of YASS. *IEEE Trans. Inform. Forensics and Security*, 4(3):369-382, Sept. 2009.

[17] M. Li, D. A. Pados, S. N. Batalama, and M. J. Medley. Passive spread-spectrum steganalysis. In *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*. Brussels, Belgium, Sept. 2011.

[18] H. S. Malvar and D. A. Florencio. Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Trans. Signal Proc.*, 51(4):898-905, Apr. 2003.

[19] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Proc.*, 6(12):1673-1687, Dec. 1997.

[20] J. Hernandez, M. Amado, and F. Perez-Gonzalez. DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Trans. Image Proc.*, 9(1):55-68, Jan. 2000.

[21] C. Qiang and T. S. Huang. An additive approach to transform-domain information hiding and optimum detection structure. *IEEE Trans. Multimedia*, 3(3):273-284, Sept. 2001.

[22] M. Barni, F. Bartolini, A. De Rosa, and A. Piva. A new decoder for the optimum recovery of nonadditive watermarks. *IEEE Trans. Image Proc.*, 10(5):755-766, May 2001.

[23] C. Fei, D. Kundur, and R. H. Kwong. Analysis and design of watermarking algorithms for improved resistance to compression. *IEEE Trans. Image Proc.*, 13(2):126-144, Feb. 2004.

[24] M. Gkizeli, D. A. Pados, and M. J. Medley. Optimal signature design for spread-spectrum steganography. *IEEE Trans. Image Proc.*, 16(2):391-405, Feb. 2007.

[25] M. Gkizeli, D. A. Pados, and M. J. Medley. SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography. In *Proc. IEEE Intern. Conf. Image Proce. (ICIP)*, pages 1561-1564. Singapore, Oct. 2004.

[26] P. Bas and F. Cayre. Achieving subspace or key security for WOA using natural or circular watermarking. In *Proc. ACM Multimedia and Security Workshop*. Geneva, Switzerland, Sept. 2006.

[27] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley. Blind iterative recovery of spread-spectrum steganographic messages. In *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, pages 11-14. Genova, Italy, Sept. 2005.

[28] D. G. Manolakis, V. K. Ingle, and S. M. Kogon. *Statistical and adaptive signal processing: Spectral estimation, signal modeling, adaptive filtering and array processing*. Boston, MA: McGraw-Hill, 2000.

[29] S. Talwar, M. Viberg, and A. Paulraj. Blind seperation of synchronous co-channel digital signals using an antenna array - part I: Algorithms. *IEEE Trans. Signal Proc.*, 44(5):1184-1197, May 1996.

[30] T. Li and N. D. Sidiropoulos. Blind digital signal separation using successive interference cancellation iterative least squares. *IEEE Trans. Signal Proc.*, 48(11):3146-3152, Nov. 2000.

[31] J. M. M. Anderson, B. A. Mair, M. Rao, and C.-H. Wu. Weighted least-squares reconstruction methods for positron emission tomography. *IEEE Trans. Medical Imaging*, 16(2):159-165, Apr. 1997.

[32] M. Li, S. N. Batalama, D. A. Pados, and J. D. Matyjas. Multiuser CDMA signal extraction. In *Proc. IEEE Military Commun. Conference (MILCOM)*. Washington D.C., Oct. 2006.

[33] M. Li, S. N. Batalama, and D. A. Pados. Population size identification for CDMA eavesdropping. In *Proc. IEEE Military Commun. Conference (MILCOM)*. Orlando, FL, Oct. 2007.

[34] J. Eriksson and M. Viberg. Asymptotic properties of nonlinear weighted least squares in radar array processing. *IEEE Trans. Signal Proc.*, 52(11):3083-3095, Nov. 2004.

[35] A. Hyvärinen and E. Oja. A fast fixed-point algorithm for independent component analysis. *Neural Computation*, 9(7):1483-1492, Oct. 1997.

[36] J. F. Cardoso. High-order contrasts for independent component analysis. *Neural Computation*, 11(1):157-192, Jan. 1999.

[37] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*, Philadelphia, PA: SIAM, 2000.

[38] *USC-SIPI Image Database*, [Online]. Available: http://sipi.usc.edu/database/database.cgi?volume=misc

# APPENDIX

## Proof of (11)

The GLS cost function in (9) can be rewritten as

$$\begin{aligned} J &= \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y} - \mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{V}\mathbf{B}\|_F^2 && (20)\\ &= \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\mathbf{V}^T\right\} - \\ &\quad \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\mathbf{V}^T\right\} && (21)\end{aligned}$$

where $\mathrm{tr}\{\cdot\}$ denotes the trace of a matrix.

For a given message matrix $\mathbf{B}$, the GLS optimal estimate of $\mathbf{V}$ can be obtain by differentiating the cost function $J$ with respect to $\mathbf{V}^T$ and setting the outcome equal to the zero matrix,

$$\frac{\partial J}{\partial \mathbf{V}^T} = -\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T + \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{B}\mathbf{B}^T) = \mathbf{0}, \quad (22)$$

$$\Rightarrow \mathbf{V} = \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \quad (23)$$

■

## Proof of (12)

We manipulate the GLS cost function in the form of (21) to write

$$\begin{aligned} J &= \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\right\} - \\ &\quad \mathrm{tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\right\}. && (24)\end{aligned}$$

Pretend that $\mathbf{V}$ is known and relax the domain of the symbol information matrix to the real space, $\mathbf{B} \in \mathbb{R}^{K\times M}$. The GLS optimal *estimate* of $\mathbf{B} \in \mathbb{R}^{K\times M}$ can be calculated again by differentiation

$$\frac{\partial J}{\partial \mathbf{B}^T} = -\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B} = \mathbf{0}, \quad (25)$$

$$\Rightarrow \mathbf{B} = (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}. \quad (26)$$

■

## Proof of (13)

Since $\mathbf{R}_{\mathrm{y}} = \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{V}\mathbf{V}^T + \mathbf{R}_{\mathrm{z}}$, by the Matrix Inversion Lemma (also known as Woodbury's Identity [37]), we can obtain

$$\mathbf{R}_{\mathrm{y}}^{-1} = \mathbf{R}_{\mathrm{z}}^{-1} - \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. \quad (27)$$

Then,

$$\begin{aligned} \mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V} &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V} - \\ &\quad \mathbf{V}^T\mathbf{R}_{z}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V} \\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}[\mathbf{I} - (\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}] \\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} \\ &\quad [(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}) - \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}] \\ &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}. && (28)\end{aligned}$$

By the property of the inverse of a product of matrices [37],

$$\begin{aligned} (\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1} &= (\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})(\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} \\ &= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} + \mathbf{I}. && (29)\end{aligned}$$

We combine the results of (27) and (29) and finally obtain

$$\begin{aligned} (\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1} &= \left((\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} + \mathbf{I}\right)\mathbf{V}^T \\ &\quad \left(\mathbf{R}_{\mathrm{z}}^{-1} - \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\right) && (30)\\ &= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. && (31)\end{aligned}$$

■